Beyond the Hype

Applying Machine Learning and Data Science to Security

Jared M. Smith

@jaredthecoder

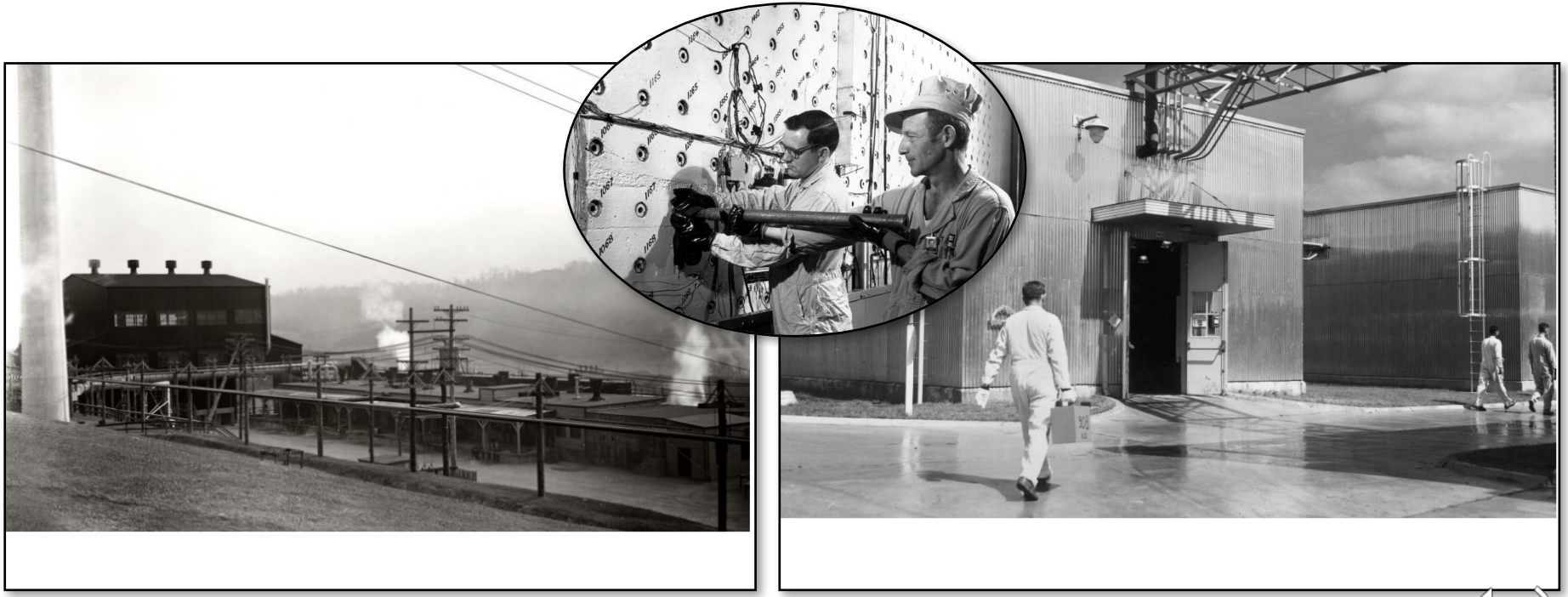
HamOntML 2017

About Me

- From Knoxville, TN
- Cyber Security Research Scientist at Oak Ridge National Lab
  - Principal Investigator for projects for the US DHS and US DOE
- BS/MS in CS from the University of Tennessee, Knoxville (UTK)
  - Current PhD Candidate at UTK
- Guest Teacher at Treehouse

ABOUT ORNL

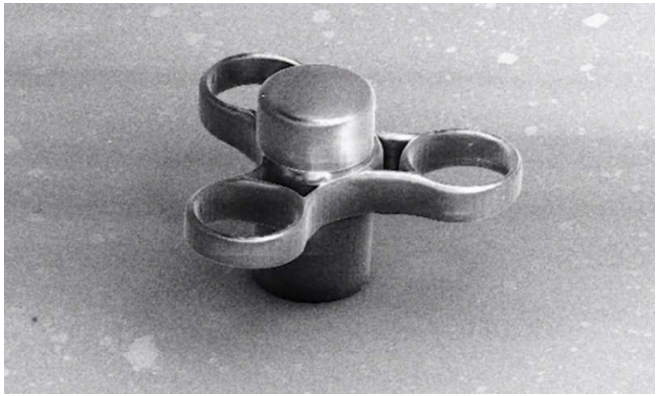
The Manhattan Project



US DOE's Largest National Lab

- First 3D printed car and house
- World's fastest supercomputer (in 2014, and again soon in 2018)
- Data warehouse of 20+ million US VA full healthcare and medical history records
- Quantum computing research facility
- Spallation Neutron Source


TITAN

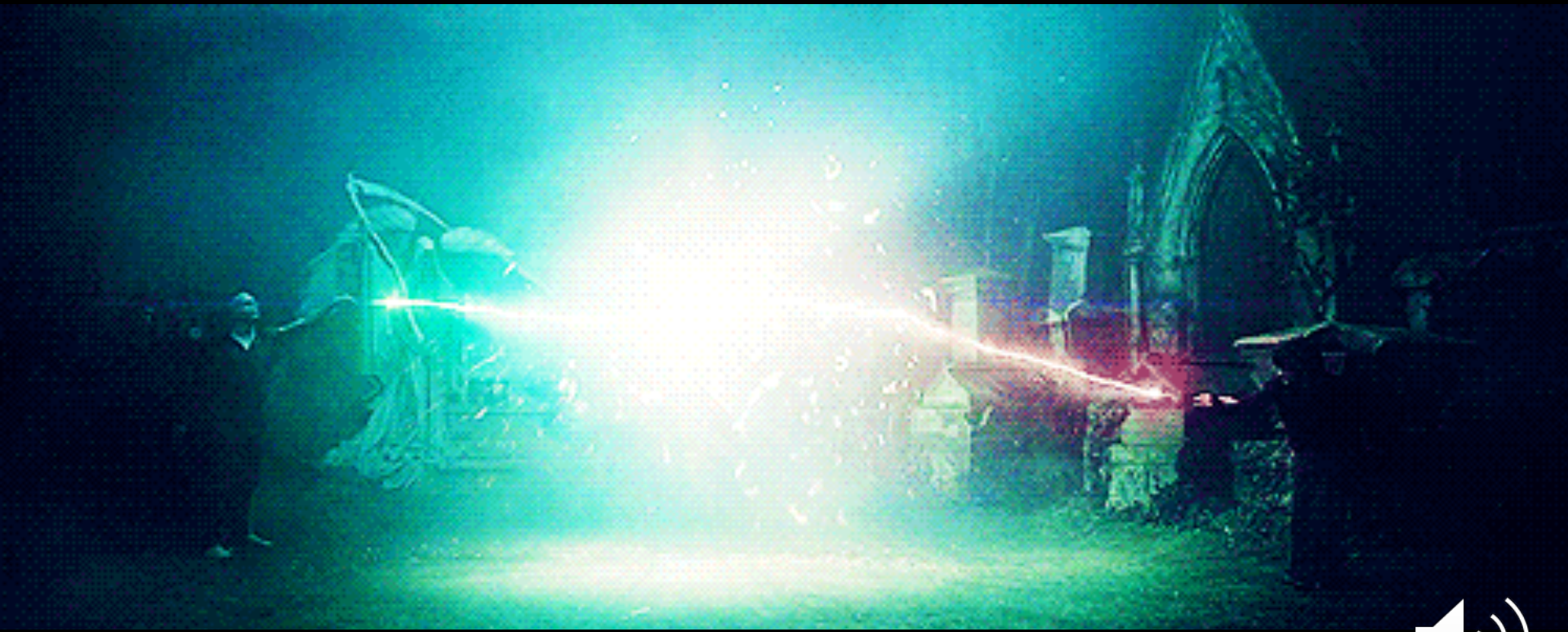


Our Research Areas

- *Power grid and SCADA/ICS security
- Formal verification of software and hardware
- Zero-day intrusion detection systems
- *Situational awareness on hosts and networks
- *Future Internet architecture security
- *Static and dynamic analysis of malware
- *Connected vehicle security and privacy
- *Automated digital forensics and incident response
- Post-Quantum cryptography
- *Deep learning for malware analysis and intrusion detection

Sponsors and Partners

[.*] SECURITY



Defense Against the Dark Arts

20 Billion

"devices" connected to the Internet in 2017

75 Billion

devices by 2025

3.8 Billion

users on the Internet in June 2017

- **What devices do we protect?** *What do we do to protect distributed systems?*
- **How do we protect and verify users?** *How do we protect networks and users running old and outdated software/hardware?*
- **How do we protect devices and users?** *How do we protect against skilled attacks?*

Choose Your Hat

- Black hats, white hats, grey hats, etc…
- Used to classify “hackers” by their motivations, purpose, compensation, and **generalized** characteristics

Motivation Matters

- It's helpful to understand how different parties are motivated
- Money, power, destruction…
- Morality, responsibility, protection of the innocent


MakeAGIF.com

White Hats

- Security researchers
- Practice “responsible disclosure”
- Participate in bug bounties
- Spread security awareness
- Maintain active Twitter accounts

Black Hats

- Motivations usually include at least one of the following:
  - Money - LinkedIn data breach
  - Power - North Korea vs. Sony
  - Destruction - Ukrainian power grid
  - Revenge - “Hacktivists”, Anonymous group

Attacker Skill Level

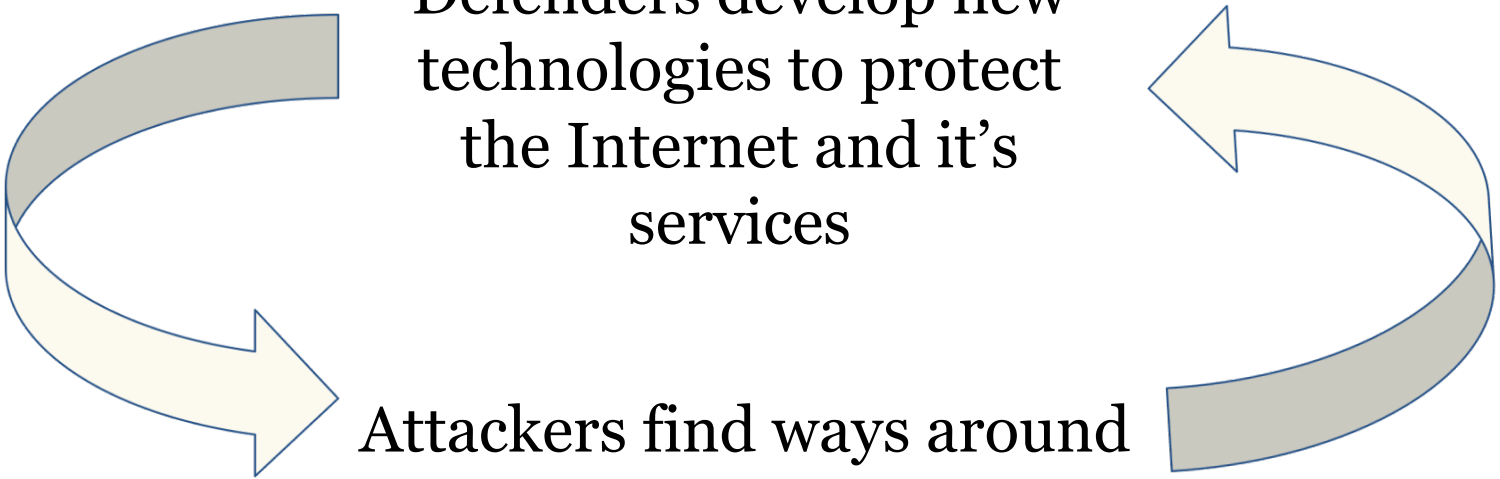
- Accidental Discovery
- The Curious Attacker
- Script Kiddies
- The Motivated Attacker
- Organized Crime
- Nation State

“War…war never changes…”

- Ulysses S. Grant

Security is and *will always be* humanity's most complex game of cat and mouse.

Vicious (or virtuous?) Circle



Many Domains

- Web Security
- Software Security
- Network and Distributed Systems Security
- Communications Security
- Cryptography
- Vehicle/Transportation Security
- Critical Infrastructure (SCADA/ICS) Security
- IoT Security
- Security Education
- Usable Security (UI/UX)
- Digital Forensics and Incident Response
- Malware Analysis
- Reverse Engineering
- Privacy and Anonymity
- Financial Security (e.g. cryptocurrencies)
- Hardware Security
- Programming Language Security
- Adversarial Machine Learning (not GANs)

To succeed in defensive *or offensive* security, you must constantly outsmart your adversary.

Since the dawn of computers, naïve security defenses have been used.

Naïve Defensive Measures

- Stateless firewalls/port blocking
  - Lacks robustness against skilled adversaries
- Inaccurate heuristics
  - 30% false positive rate is not okay in security
- Whitelisting and blacklisting IPs, users, domains, etc.
  - Hardcoded and doesn't adapt, costly to performance

Offense lacks robustness too!

Naïve Offensive Measures

- Malware that reuses code of other malware
  - Easy to detect by simple comparison
- Automated port scanning
  - Often scans without mimicking a real user
- Manual vulnerability discovery
  - Extremely complex systems cannot be analyzed in full manually

The recent growth in quality, tooling, and community support in data science has opened major opportunities to data scientists looking to make an impact in security.

ML-enabled Defense

- **Offense:** “Undetectable” malware
- **Counter-Measure:** Generative Adversarial Networks can trained against random variations of malware samples

- **Offense:** Exploit poorly designed (UI/UX) security features to steal data from users
- **Counter-Measure:** Data-driven approach to usability

- **Offense:** Security analysts/sysadmins overwhelmed with signals
- **Counter-Measure:** Provide data-driven tools to comb through the mess of alerts, dashboard, Slack messages, and documents.

ML-enabled Offense

- **Defense:** Vehicle Tech Obscurity
- **Counter-Measure:** Anomaly detection on the CAN bus

- **Defense:** ML-based packet filtering or spam detection
- **Counter-Measure:** Adversarial ML

- **Defense:** Bot detection heuristics to prevent web scraping, click-farming, etc.
- **Counter-Measure:** Constantly learning near-human bots

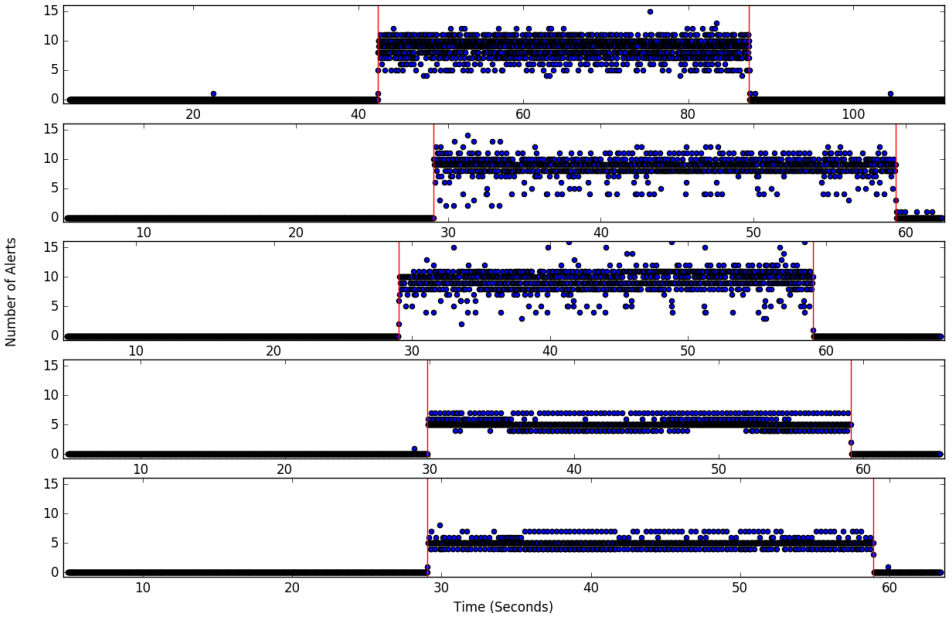
Case Studies

In-Vehicle Network Anomaly Detection

- Vehicles have around 150 control units broadcasting critical signals over a centralized CAN bus
- Vulnerabilities can be exploited via OBD-II ports, USB, AUX ports, Bluetooth, Wi-Fi, etc.
- Using standard statistical inference methods, CAN bus signal frequencies can be monitored and analyzed

In-Vehicle Network Anomaly Detection

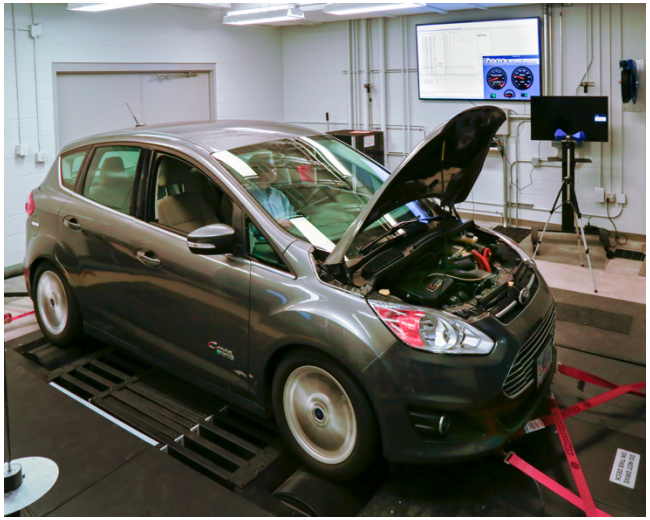
- Requires only five seconds of training time (on normal data)
- Achieved true positive and false negative rates of 0.9998/0.00298, respectively



Michael R. Moore, Robert A. Bridges, Frank L. Combs, Michael S. Starr, and Stacy J. Prowell. 2017. Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks: a data-driven approach to in-vehicle intrusion detection. In *Proceedings of the 12th Annual Conference on Cyber and Information Security Research* (CISRC '17)

In-Vehicle Network Anomaly Detection

- More complex approaches could see better results
  - Time series prediction with recurrent neural networks
- Similar work is being done for larger vehicles, from trucks to tanks
- Vehicle security is in its early stages, with testbeds still largely unavailable



Adversarial ML

- Deep learning works really well
- Except when it doesn't…

Whale

Turtle

DeepFool: a simple and accurate method to fool deep neural networks. 2016 CVPR.

Adversarial ML

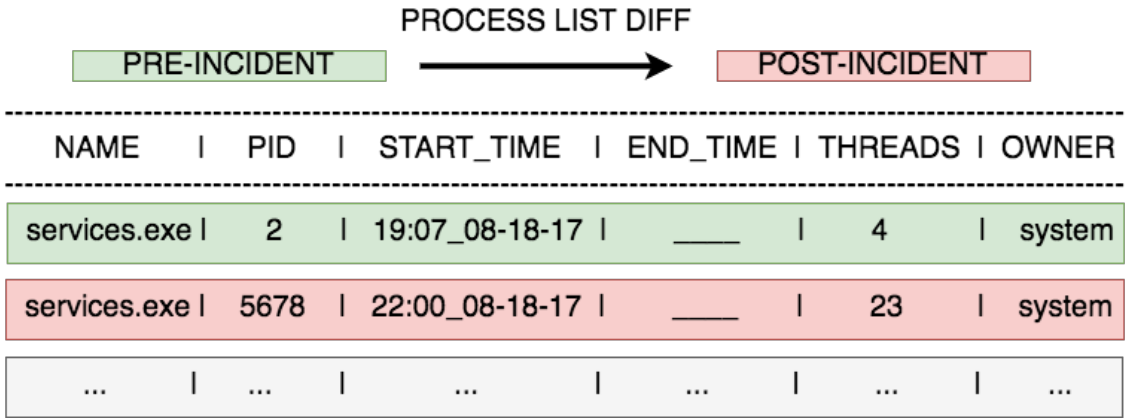
- This works against CNNs, RNNs, and most standard algorithms not pre-trained to be robust
- For more: *https://github.com/yenchenlin/awesome-adversarial-machine-learning*

Host-based Forensic Analysis

- **Problem:** How do we get insight into the spread of malware across a machine(s)?
- **Approach:** Gather host data before, during, and after potentially noteworthy alerts, and analyze the difference over time
  - Running processes, user information, loaded code libraries (DLLs), networking data, etc.

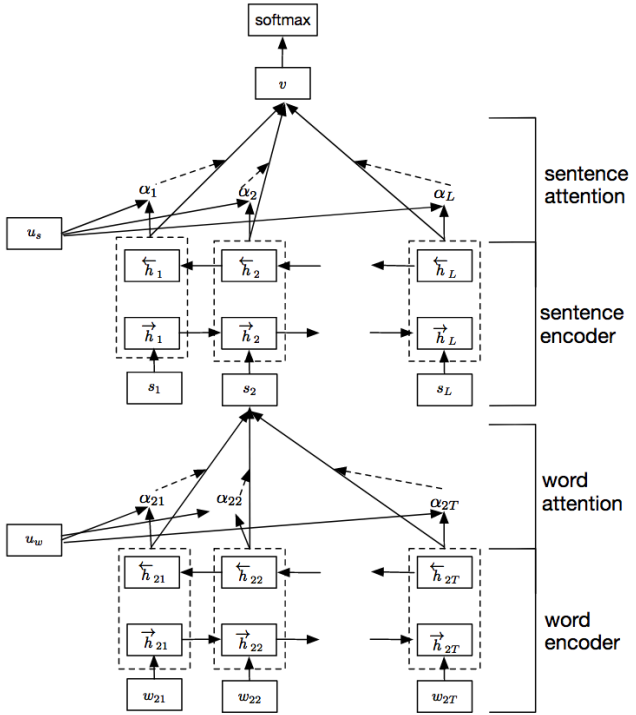
Host-based Forensic Analysis

- Using snapshots over time, diff the state at each point, and use machine learning to tell whether they are malicious snapshots (i.e. represent an infection)



Host-based Forensic Analysis

- Need to capture many time-series snapshots for machines that **are infected** and **not infected**
- Could use existing NLP to analyze text
- Or newer deep-learning based approaches → *Hierarchical Attention Networks*



Jared M. Smith, Elliot Greenlee, and Aaron Ferber. 2017. Akatosh: Automated Cyber Incident Verification and Impact Analysis. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (CCS '17).

Additional Links

- http://www.covert.io/
- http://datadrivensecurity.info/blog/
- https://www.mlsecproject.org/
- http://www.automatingosint.com/blog/
- https://bigsnarf.wordpress.com/
- https://github.com/jivoi/awesome-osint
- https://github.com/rshipp/awesome-malware-analysis
- https://github.com/jaredthecoder/awesome-vehicle-security

Thanks to…

- Ken Sills and Preteckt for inviting me to speak!
- The people of Hamilton for making me feel welcome!

Questions?

 jaredthecoder.com

 jaredthecoder

 jaredthecoder

 jaredthecoder

 jared@jaredthecoder.com